# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/304,444 | 05/03/1999 | GREGORY BURNS | MS1-301US | 9671 |

22801          7590          04/26/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

| EXAMINER |
|---|
| KLIMACH, PAULA W |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 04/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on _07 April 2004_.

2a)☐ This action is **FINAL**.        2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
  closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) _1-19_ is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-19_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All   b)☐ Some * c)☐ None of:

  1.☐ Certified copies of the priority documents have been received.

  2.☐ Certified copies of the priority documents have been received in Application No. _____.

  3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
    application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
  Paper No(s)/Mail Date _4_.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1.      This office action is in response to amendment filed on 4/07/04 (Paper No. 10). Original

application contained Claims 1-19. Applicant amended Claim 7. The final rejection of the

1/13/2004 Office Action (Paper No.8) has been withdrawn. The amendment filed on 4/07/04

have been entered and made of record. Therefore, presently pending claims are 1-19.

### *Response to Arguments*

2.      Applicant's arguments filed 4/07/04 have been fully considered but they are not

persuasive because of following reasons.

Applicant argued, "Hayes teaches a client-server environment, wherein a user's profile is

not even stored on the user's own (client) computer, but are in fact stored remotely, on the

network server". This is not found persuasive. Hayes teaches the idea of a person's profile being

accessible on any computer that they decide to log onto. In the combination of Jones and Hayes,

the portable storage device would perform the function of the central computer by providing the

profile at any computer that the user decides to log onto by manually transferring the

information. Jones also teaches the increased security of being able to detach the memory device

in order to transport the data (column 3 lines 33-36).

The examiner asserts that the prior art does teach or suggest the subject matter broadly

recited in independent Claims 1, 5, 7, 11, 15, and 17-19. Dependent Claims 2-4, 6, 8-10, 12-14,

and 16 are also rejected at least by virtue of their dependency on independent claims and by

other reason set forth in this office action (Paper No. 11). Accordingly, rejections for claims 1-19

are respectfully maintained.

*Claim Rejections - 35 USC § 102*

3.      The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(b) the invention was patented or described in a printed publication in
> this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application
> for patent in the United States.

4.      **Claim 1, 7, and 17** are rejected under 35 U.S.C. 102(b) as being anticipated by Jones

(5,623,637).

*In reference to claims 1 and 7,* Jones discloses a system for safely porting user data from

one computer to another (column 1 lines 60-65), comprising: a memory device to store the user

data (part 100 of Fig. 1 in combination with column 1 lines 15-45); and a smart card (part 250 of

Fig. 1 in combination with column 4 lines 59-65). The smart card is associated with a user

because the user must know that password stored in the smart card for the smart card to release

the information stored in the removable memory (column 3 lines 40-43 in combination with

column 4 lines 59-67 in combination with column 5 lines 54-67). The smart card alternately

enables access to the user data on the memory device when both the memory device and smart

card are interfaced with a common computer and disables access to the user data when one of the

memory device or smart card is absent (column 4 lines 47-67). The data from the PCMCIA card

is only made available to the host if the enable signal is transmitted from the smart card;

therefore the smart card and the host have to be at the same host. Access is disabled when the

signal is not received.

*In reference to claim 17,* this claim differs from claim 1 because of storing access

credentials on a smart card the access credentials enabling access to the user data stored on the

portable memory device. The password stored on the smart card would be equivalent to the

access credentials (column 5 lines 42-53).

*In reference to claims 3 and 8*, Jones disclose a password (passcode) stored on a smart

card and access to user data in the memory device being enabled upon authentication of a user-

supplied passcode to the passcode stored on the smart card (column 5 lines 54-67). A password,

as defined by the Webster's dictionary, is something that enables one to pass or gain admission.

Therefore, the pass code is a type of password. The comparing of the password entered by the

user with the password stored in the smart card is a form of authenticating the smart card.

### Claim Rejections - 35 USC § 103

5.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

6.      **Claims 4, 9, and 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones

as applied to claim 1 and 7 respectively above.

The system wherein the memory device stores a public key and the smart card stores a

corresponding private key and access to the user data in the memory device is enabled upon

verification that the public key and the private key are associated.

Jones discloses the smart card I.C storing a private key from the corresponding public

key for a remote computer. Access is enabled upon verification that the public key and the

private key are associated (column 9 lines 22-37 in combination with column 9 lines 5-15).

Jones does not expressly disclose the PCMCIA card storing the public key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the public key in the PCMCIA card. One of ordinary skill in the art would have been motivated to do this because the information in the PCMCIA card is being protected just as the information in the remote computer is protected.

7.      **Claim 2, 5-6, 11-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones as applied to claim 1 above, and further in view of Hayes et al (20010011341).

*In reference to claim 2*, Jones does not expressly disclose a system wherein the memory device stores a user profile that can be used to configure a computer.

Hayes discloses a user profile that is kept in the user's computer and used to configure the user's computer, page 1 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user's profile described by Hayes in memory device disclosed by Harari.

One of ordinary skill in the art would have been motivated to do this because user would be required to identify themselves and, therefore gain access permission or not, Hayes page 2 paragraph 12.

*In reference to claim 5*, Jones discloses a system comprising of a smart card and a memory device (part 100 of Fig. 1 in combination with column 1 lines 15-45 in combination with part 250 of Fig. 1 in combination with column 4 lines 59-65). Jones disclose a password (passcode) stored on a smart card and access to user data in the memory device being enabled

upon authentication of a user-supplied passcode to the passcode stored on the smart card (column

5 lines 54-67). The memory device and the smart card in the system disclosed by Jones are

interface with a common computing unit (column 4 lines 47-67). The data from the PCMCIA

card is only made available to the host if the enable signal is transmitted from the smart card;

therefore the smart card and the host have to be at a common host. Jones discloses a password

stored on a smart card (column 5 lines 54-67). In addition Jones teaches of a remote device with

a public key and a local device connected to a smart card that contains the private key, column 9

lines 24-42. The information stored on the local device can be stored on the smart card and the

information on the remote device can be stored on the memory device. The user data would then

only be made accessible when the correct private key and public key pair are applied. (The

smart card is an integral part of the memory device).

Hayes discloses a user profile that is stored on a computer.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to store the user profile disclosed by Hayes in the memory system disclosed by

Jones. One of ordinary skill in the art would have been motivated to do this because functions

that were previously performed within the confines of a secure office space are now done in the

field (Jones column 1 lines 15-32). The system disclosed by Hayes would provide a method of

saving the user's configuration in a central place so that the user may reproduce the preferences

chosen earlier (page 2 paragraph 0012). The portable storage device disclosed by Jones would

be the central place.

*In reference to claim 6*, the memory device of Jones interfaces with the Host using a standard PCMCIA interface (column 4 lines 1-10). The UART performs that tasks of the smart card reader (part 230 Fig. 1).

*In reference to claim 11*, Jones discloses a system as in the rejection for claim 1.

However, Jones does not disclose a memory device to store the user's profile.

Hayes discloses a user's profile being stored in memory wherein the profile is accessible to configure the computer (page 1 paragraph 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to save the user's profile described by Hayes in the memory device described by Jones.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission, Hayes page 2 paragraph 12.

*In reference to claim 12*, Jones disclose a password (passcode) stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card (column 5 lines 54-67). A password, as defined by the Webster's dictionary, is something that enables one to pass or gain admission. Therefore, the pass code is a type of password. The comparing of the password entered by the user with the password stored in the smart card is a form of authenticating the smart card.

*In reference to claim 13*, Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The information stored on the local device can be stored on the smart card and the information on the

remote device can be stored on the memory device. The user data would then only be made

accessible when the correct private key and public key pair are applied.

*In reference to claim 14,* Jones discloses a system where the IC card (smart card) stores a

passcode (column 5 lines 54-67). Jones teaches of a remote device with a public key and a local

device connected to a smart card that contains the private key, column 9 lines 24-42. The

information stored on the local device can be stored on the smart card and the information on the

remote device can be stored on the memory device. The user data would then only be made

accessible when the correct private key and public key pair are applied.

*In reference to claim 15,* Jones discloses a computer system as in the rejection of claim 1.

Jones does not disclose a system for storing a user's profile for configuring the computer.

Hayes discloses a system where the user's profile is stored in memory for access for

configuring the computer, page 1 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to store the user profile, for configuring the computer that was described by

Hayes, in the smart card secured memory system, described by Jones.

One of ordinary skill in the art would have been motivated to do this because it is

desirable that the user identify themselves before gaining access permission, Hayes page 2

paragraph 12.

*In reference to claim 16,* Jones discloses the computer system as applied to claim 15.

Jones further discloses a system where data can be securely transported from one computer to a

second computer (column 14 lines 20-30).

8.     **Claims 18 and 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones

and Hayes in view of Sigbjørnsen et al US 6,266,416 B1.

Jones discloses a system that stores user data in a portable memory device (column 1

lines 60-65). The PCMCIA card interfaces with the computer (column 4 lines 1-5). The smart

card interfaces with the computer using the UART (Fig. 1 part 230). Jones discloses the smart

card I.C storing a private key from the corresponding public key for a remote computer. In

order, to protect information stored in the PCMCIA card the public key should be stored in the

PCMCIA card as it was stored in the remote computer. Jones discloses a password stored in the

smartc card (Fig. 3 part 420). The system permits use of the card-residnet key following

validation of the user-entered passcode with the passcode stored in the smart card (column 5

lines 54-67). The card resident key and the device resident key are authenticated (column 9 lines

5-20). Access is enabled upon verification that the public key and the private key are associated

(column 9 lines 22-37 in combination with column 9 lines 5-15).

Sigbjørnsen teaches of a system where an asymmetric authentication key is transferred to

the smart card and decrypted in the smart card to initiate an authentication process in the smart

card, column 7 lines 44-49.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art would use the system to store the password and a key on the smart card, store a

corresponding key on the memory device, and transmitting the stored key from the memory

device to the smart card in order to carryout the authentication.

One of ordinary skill in the art would have been motivated to do this because storing the

password and a key on the smart card and a corresponding key on the memory device would

increase the security by requiring the user to be in possession of the memory card (which has the

required keys) and the password, Jones column 9 lines 55-60. Carrying out authentication on the

smart card give the users complete portability, user authentication can be carried out across

operating systems and multiple computers.
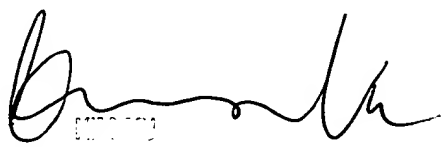
### *Conclusion*

9.      Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, April 19, 2004